



CENTERS for MEDICARE & MEDICAID SERVICES

Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850



**Risk Management Handbook
Volume II
Procedure 3.3**

Common Control Identification

**FINAL
Version 1.0
June 25, 2014**

Document Number: CMS-CISO-2014-vII-pr3.3

(This Page Intentionally Blank)

**SUMMARY OF CHANGES IN *COMMON CONTROL IDENTIFICATION*, VERSION
1.0**

1. Baseline Version

(This Page Intentionally Blank)

TABLE OF CONTENTS

1 OVERVIEW.....1

1.1 Purpose..... 1

1.2 Other Relevant Publications 1

1.3 Inherited Controls List..... 1

2 COMMON CONTROL IDENTIFICATION PROCEDURE2

2.1 Identifying Inheritable Controls..... 2

 2.1.1 Procedure Users 2

 2.1.2 Initial Conditions 3

 2.1.3 Identifying Inheritable Controls..... 4

3 APPROVED11

LIST OF TABLES

Table 1 Sample Inherited Controls List 2

(This Page Intentionally Blank)

1 OVERVIEW

1.1 PURPOSE

The purpose of this procedure is to provide CMS business owners, System Developer/Maintainers, Information System Security Officers, and other CMS personnel with the necessary procedures to identify any security controls that the system may inherit, called common controls.

Use this procedure during the *Concept Phase* of a project. Early identification of inheritable controls during the system life cycle can reduce the number of controls that a system must implement and test. This can result in lower project cost, shorter project schedules, and reduced operational security control maintenance and testing costs. Perform this procedure for all conceptual *alternatives* that are under consideration for a new system. This improves project cost and time estimates and facilitates comparison of both project cost and total cost of ownership among candidates.

1.2 OTHER RELEVANT PUBLICATIONS

Other relevant *Risk Management Handbook (RMH)* publications include:

- RMH Volume I, Chapter 1, *Risk Management in the XLC*. This chapter provides information required to understand the interrelation of information security, risk management, and the system life cycle.
- RMH Volume II, Procedure 2.3, *Categorizing an Information System*. This procedure is required to establish the security category of the system. All controls that a system inherits must meet or exceed the requirements for the established category.

All applicable RMH procedures are available on the CMS information security website, in the *Information Security Library* at: <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>.

1.3 INHERITED CONTROLS LIST

Projects have flexibility in how to perform the comparative analysis that results in determination of the preferred alternative. An inherited controls list can be used to identify common controls offered by each system alternative. In addition, it can specify if the common control provides the required protection fully (with nothing further needed from the system or its owners) or in hybrid fashion (partially by the alternative, with the remainder provided by the system and its owner). Note: Non-inheritable controls must be built during the project and implemented as part of the system.

The format of inherited controls lists is optional, projects should use one that identifies and compares significant differences among alternatives effectively for the project. It could resemble the list that is partially depicted in Table 1. However, the objective of this processes is to

identify opportunities to extract benefits (and reduce costs) by maximizing the use of already existing solutions, and minimizing duplication of efforts across the enterprise.

Table 1 Sample Inherited Controls List

Item	Control	Description	Alt 1	Alt 2	Alt 3	Alt 4
...						
17	CM-5	Access Restrictions for Change	Hybrid			
18	CM-6	Configuration Settings	Hybrid		Full	Hybrid
...						
23	PE-13	Fire Protection	Full		Hybrid	
...						

It should be noted that *coordination* and *understanding* of the interface between the applicable controls (applicable control *providers* and various alternative control *inheritors*) is required before any real *value* can be achieved from this process. It is therefore imperative that communications and discourse (to clarify understanding of various control inheritances) occur between these provider/inheritor entities before any *final* alternative solutions are selected.

2 COMMON CONTROL IDENTIFICATION PROCEDURE

PROCEDURE

PRINCIPLE

2.1 IDENTIFYING INHERITABLE CONTROLS

2.1.1 PROCEDURE USERS

1. CMS Information System Security Officer (ISSO).
2. Business Partner System Security Officer (SSO).
3. Business Owners.
4. System Developer/Maintainers.

PROCEDURE

PRINCIPLE

5. Other CMS personnel responsible for defining work or costs for projects.

2.1.2 INITIAL CONDITIONS

1. The system security category was established in accordance with RMH Volume II, Procedure 2.3, *Categorizing an Information System*.

2. Project *alternatives* (candidates) have been identified.

*The planning segment of the Initiation, Concept, and Planning Phase of the XLC is a pivotal point for projects. During this segment, evaluations of various **alternatives** for the proposed system against requirements result in development of project cost and time estimates, including those that are security-related. The estimates include both project and ongoing system cost. See RMH Volume 1, Chapter 1, Risk Management in the XLC for more information.*

PROCEDURE

PRINCIPLE

**2.1.3 IDENTIFYING
INHERITABLE
CONTROLS**

NOTE:

This procedure contains the steps to identify inheritable controls for conceptual *alternatives* (candidate vendor, operating-site, platform, organizational-environment, etc.) Apply this procedure for *each* conceptual *alternative* that is under evaluation.

1. If the system will operate within an *infrastructure* (data center) that has a current CMS *Authorization to Operate (ATO)*, perform the following:

a. Contact the applicable *infrastructure* (data center) ISSO to obtain a list of inheritable controls, including scope, qualifications, and restrictions.

b. Evaluate the data center response to identify appropriate inheritable controls. For *each* candidate inheritable control:

(1) Assess and evaluate that the available inheritable control meets the following objectives:

(a) The inheritable control is *appropriate* to the candidate *alternative*.

See Initial Conditions (Section 2.1.2, Step 2 above).

There may be controls that can be inherited from this data center.

Inheritable Controls must be operational, pass assessments, and apply to the system that wants to use them. If not, use or create a system-specific control, or develop a plan (Plan of Action and Milestones [POA&M]) for supplementing the inheritable control into compliance.

Example: An offered multi-factor authentication control may only be appropriate for application-access through a Virtual Private Network (VPN) access-point from the internet (via an RSA™ token.) If the candidate alternative is not accessing through that VPN portal infrastructure, then control inheritance is not possible.

PROCEDURE

PRINCIPLE

(b) Is currently in operation and available to the candidate *alternative*.

*Controls that are not **fully** in operation (i.e., proposed or under development) are not suitable for use in a new implementation.*

(c) Is compliant with the applicable control requirement at the required security level for the candidate *alternative*.

Controls that fail to meet their design objectives (i.e. are not effective) are not suitable for use in a new implementation.

(d) Meets business objectives of the candidate *alternative*.

Example: Data centers routinely create backups of data. However, the business must define the Maximum Tolerable Downtime (MTD) and Recovery Point Objective (RPO) to evaluate if the backup services provided by the data center are adequate. If not, implement a system specific control instead.

(e) Assess and verify that the scope-of-work necessary to implement this control is feasible for the candidate *alternative*.

Each inheritable control implementation will usually require some architectural baseline design at the inheriting system (e.g., UNIX OS only, or WebSphere-compatible only, etc.). If the conceptual design of the candidate alternative does not allow for that baseline architectural design-requirement, then control inheritance is not possible.

(2) For each inheritable control that **meets all** of the objectives above:

NOTE:

The vast majority of these inheritable controls will only address a *portion* of the candidate conceptual-alternative's needs. Additional system-specific implementation resources will usually (*almost always*) be required to **fully meet the objectives of any given control requirement.**

*Example: While an inheritable Database Management System (DBMS) may provide a significant amount of access control and segregation of duties capability—it is **always** incumbent upon the local system developer/maintainer to design and implement the user roles, and dictate their associated roll-based functionality.*

(a) Add the verified-inheritable control to an inherited controls list for the applicable conceptual *alternative*.

This list is a tool to be used to compare the different conceptual alternatives. Conceptual alternatives that maximize the overall use of existing inheritable controls will typically have lower project cost and lifecycle maintenance costs.

PROCEDURE

PRINCIPLE

2. If the system will utilize *services* that have a current CMS Authorization to Operate and provide inheritable controls, perform the following:

a. Contact the applicable *services* ISSO to obtain a list of inheritable controls, including scope, qualifications, and restrictions.

b. Evaluate the *services* response to identify appropriate inheritable controls. For *each* candidate inheritable control:

(1) Assess and evaluate that the available inheritable control meets the following objectives:

(a) The inheritable control is *appropriate* to the candidate *alternative*.

(b) Is currently in operation and available to the candidate *alternative*.

(c) Is compliant with the applicable control requirement at the required security level for the candidate *alternative*.

(d) Meets business objectives of the candidate *alternative*.

Some controls may be inheritable from services.

Inheritable Controls must be operational, pass assessments, and apply to the system that wants to use them. If not, use or create a system-specific control, or develop a plan (Plan of Action and Milestones [POA&M]) for supplementing the inheritable control into compliance.

Example: An offered inheritable control may only be appropriate for systems running on a mainframe environment. If the candidate alternative is not mainframe-based, control inheritance is not possible.

*Controls that are not **fully** in operation (i.e., controls that are proposed or under development) are not suitable for use in a new implementation.*

Controls that fail to meet their design objectives (i.e. are not effective) are not suitable for use in a new implementation.

Example: A business requirement may specify a need for Internet access to a candidate alternative. If an offered inheritable access control service does not address Internet access (i.e., only offers access control for local network access), then it may not be suitable for use in a candidate alternative.

PROCEDURE

(e) Assess and verify that the scope-of-work necessary to implement this control is feasible for the candidate *alternative*.

(2) For each inheritable control that *meets all* of the objectives above:

NOTE:

The vast majority of these inheritable controls will only address a *portion* of the candidate conceptual-alternative’s needs. Additional systems-specific implementation resources will usually (*almost always*) be required to *fully* meet the objectives of any given control requirement.

(a) Add the verified-inheritable control to an inherited controls list for the applicable conceptual *alternative*.

3. If the system will utilize a CMS-authorized **Cloud Service Provider (CSP)** that, with a current CMS ATO, perform the following:

a. Contact the applicable **CSP** ISSO to obtain a list of inheritable controls, including scope, qualifications, and restrictions.

PRINCIPLE

Each inheritable control implementation will usually require some architectural baseline design at the inheriting system (e.g., Oracle DBMS, or requires the integration of some other CMS service such as the Remote Identity Proofing [RIDP] system, etc.). If the conceptual design of the candidate alternative does not allow for that baseline architectural design-requirement, then control inheritance is not possible.

Example: While an inheritable Enterprise Identity Management (EIDM) service may provide sufficient E-authentication Level authentication (necessary for meeting ARS requirement IA-8), but it may not address authentication utilizing Personal Identity Verification card [PIV Card] (necessary for meeting HSPD-12 and ARS requirement IA-2). Therefore, it is still incumbent on the candidate alternative to address the remaining authentication requirements under IA-2.

There may be inheritable controls provided by this CSP.

PROCEDURE

PRINCIPLE

b. Evaluate the *CSP* response to identify appropriate inheritable controls. For *each* candidate inheritable control:

(1) Assess and evaluate that the available inheritable control meets the following objectives:

(a) The inheritable control is *appropriate* to the candidate *alternative*.

(b) Is currently in operation and available to the candidate *alternative*.

(c) Is compliant with the applicable control requirement at the required security level for the candidate *alternative*.

(d) Meets business objectives of the candidate *alternative*.

(2) Assess and verify that the scope-of-work necessary to implement this control is feasible for the candidate *alternative*.

Inheritable Controls must be operational, pass assessments, and apply to the system that wants to use them. If not, use or create a system-specific control, or develop a plan (Plan of Actions and Milestones [POA&M]) for supplementing the inheritable control into compliance.

Example: A CSP-offered access control may only be appropriate for access to the cloud management area of the cloud—necessary for administering the application. It may not be usable for managing user-access to the application.

*Controls that are not **fully** in operation (i.e., controls that are proposed or under development) are not suitable for use in a new implementation.*

Example: If the business requires extensive use and storage of PHI or PII, those data-types present additional Federal requirements for storage, access controls, and auditing, etc. (over and above the baseline FedRAMP requirements.) If the proposed CSP controls do not account for these additional PII/PHI requirements, the CSP may not be suitable for use—at least not for the part of the candidate alternative that deals directly with PHI/PII.

Example: Cloud services typically are well suited for universal access to an application (usually via the Internet). However, clouds are not always well-suited (from a cost-perspective) for high-volume data transactions with high network traffic.

PROCEDURE

(3) For each inheritable control that *meets all* of the objectives above:

NOTE:

The vast majority of these inheritable controls will only address a *portion* of the candidate conceptual-alternative’s needs. Additional systems-specific implementation resources will usually (*almost always*) be required to *fully* meet the objectives of any given control requirement.

(a) Add the verified-inheritable control to an inherited controls list for the applicable conceptual *alternative*.

4. If the system will fall within the scope of an *organization* that is an authorized CMS common control provider, perform the following:

a. Contact the applicable *organization* ISSO to obtain a list of inheritable controls, including scope, qualifications, and restrictions.

PRINCIPLE

*Example: While a cloud-based database may provide a significant amount of access control and segregation of duties capability—it is **always** incumbent upon the customer (CMS) developer/maintainer to design and implement the user roles, and manage their associated roll-based functionality.*

There may be inheritable controls provided by this organization.

PROCEDURE

PRINCIPLE

b. Evaluate the *services* response to identify appropriate inheritable controls. For *each* candidate inheritable control:

(1) Assess and evaluate that the available inheritable control meets the following objectives:

(a) The inheritable control is *appropriate* to the candidate *alternative*.

(b) Is currently in operation and available to the candidate *alternative*.

(c) Is compliant with the applicable control requirement at the required security level for the candidate *alternative*.

(d) Meets business objectives of the candidate *alternative*.

(2) Assess and verify that the scope-of-work necessary to implement this control is feasible for the candidate *alternative*.

Inheritable Controls must be operational, pass assessments, and apply to the system that wants to use them. If not, use or create a system-specific control, or develop a plan (Plan of Actions and Milestones [POA&M]) for supplementing the inheritable control into compliance.

Example: An offered organizational Human Resources control may only be appropriate to Federal employees. If the candidate alternative is proposing to use contractor personnel exclusively, those controls are not appropriate for use.

Furthermore, if the candidate alternative involves using both federal and contractor employees, those controls are valid only for the federal employees. A system specific portion of the controls must be developed for contractor personnel.

*Controls that are not **fully** in operation (i.e., proposed or under development) are not suitable for use in a new implementation.*

Controls that fail to meet their design objectives (i.e. are not effective) are not suitable for use in a new implementation.

Example: If the business objective requires the security-vetting of contractor personnel, then utilizing a personnel-vetting capability offered through the CMS Office of Operations Management (OOM)—that may vet only Federal Employees—may not meet the business objective.

PROCEDURE

(3) For each inheritable control that *meets all* of the objectives above:

NOTE:

The vast majority of these inheritable controls will only address a *portion* of the candidate conceptual-alternative's needs. Additional systems-specific implementation resources will usually (*almost always*) be required to *fully* meet the objectives of any given control requirement.

(a) Add the verified-inheritable control to an inherited controls list for the applicable conceptual *alternative*.

PRINCIPLE

Example: Physical And Environmental Protection (ARS PE family) solutions managed by OOM only apply to Federal facilities. Additional control solutions will be required at any contractor facilities within the scope of the candidate alternative.

3 APPROVED

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at <mailto:ciso@cms.gov>.

(This Page Intentionally Blank)